KARCZ Polska

# Router GSM MIDGE

(Ma zastosowanie również do MG102i)

# Analiza ruchu sieciowego / Wireshark

Wersja oprogramowania:

3.6.40.109

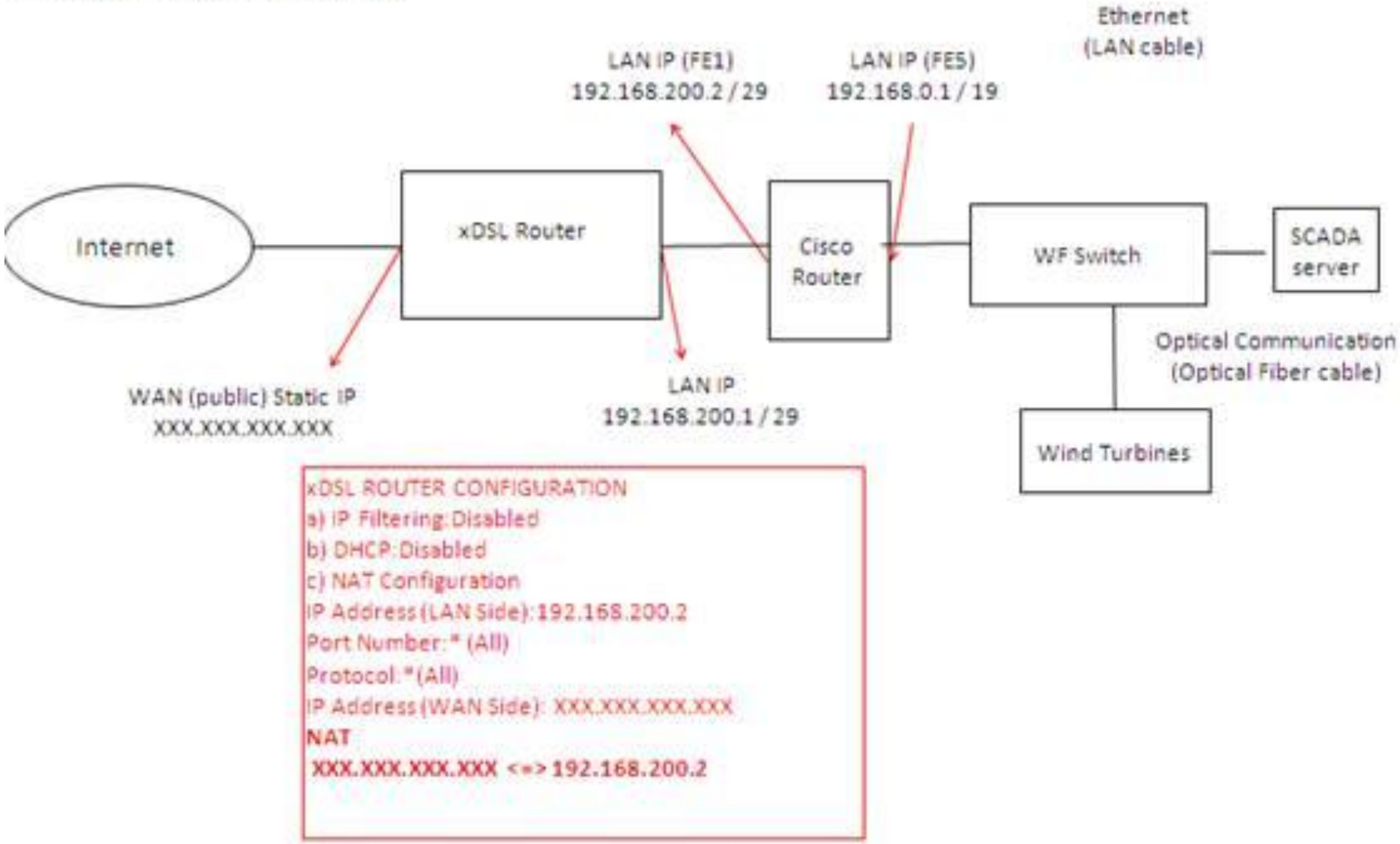
| | | | |
|---|---|---|---|
| Data dokumentu: | 13 marca 2014 | Aktualizacja: 3.02.2014r | Wersja 1.2 |
| Przygotował: | Jan Batycki | support@karczpolska.pl | 61 827 30 90 |
| Zweryfikował: | Krzysztof Karcz | support@karczpolska.pl | 61 827 30 90 |

## Analiza ruchu sieciowego M!DGE/Wireshark, sprawdzanie portu komunikacyjnego.

W routerach **M!DGE/MG102i** mamy do dyspozycji bardzo ciekawą funkcję służącą do analizy ruchu w sieci. Narzędzie **tcpdump**. Generuje ono pliki PCAP (przechwytywania sieci) które możemy później analizować programem **Wireshark** (http://www.wireshark.org/).
Dokumentacja do programu dostępna http://www.wireshark.org/docs/wsug_html_chunked/

W poniższym przykładzie przedstawię opis rozwiązania problemu u naszego klienta. Router **M!DGE** dostarcza Internet, za routerem znajduje się drugi router CISCO obsługujący zabezpieczoną sieć VPN. Za routerem CISCO znajdują się urządzenia sieciowe. Problemem był brak informacji ze strony klienta na jakich portach pracuje VPN i CISCO. Rozwiązaniem było przekierowanie całego ruchu sieciowego z M!DGE na CISO, jednak pozbawiało nas to możliwości kontroli i konfiguracji routera M!DGE, np. uruchomienia dodatkowych usług diagnostycznych dla Klienta.

**SCADA network configuration**



xDSL ROUTER CONFIGURATION

a) IP Filtering:Disabled

b) DHCP:Disabled

c) NAT Configuration

IP Address (LAN Side):192.168.200.2

Port Number:* (All)

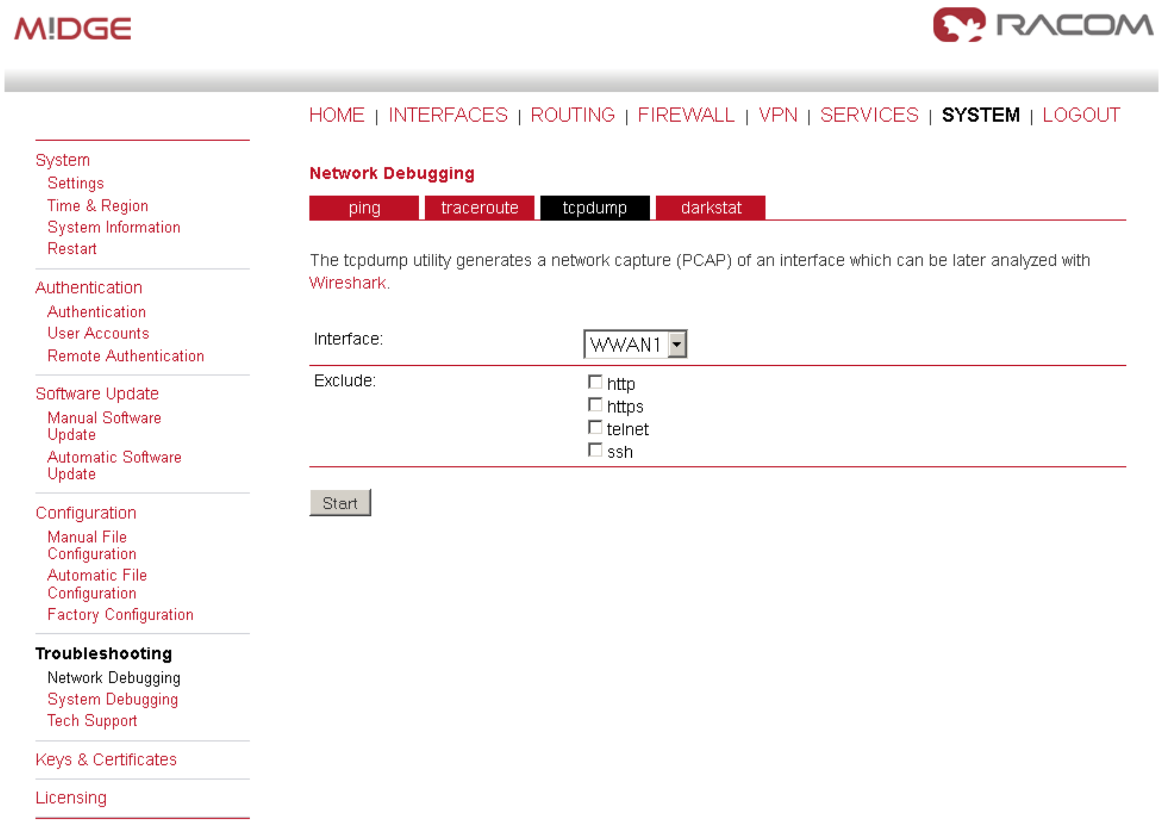
Protocol:*(All)

IP Address (WAN Side): XXX.XXX.XXX.XXX

**NAT**

**XXX.XXX.XXX.XXX <=> 192.168.200.2**

Rys.: Konfiguracja sieci u klienta



**Network Debugging**

The tcpdump utility generates a network capture (PCAP) of an interface which can be later analyzed with Wireshark.

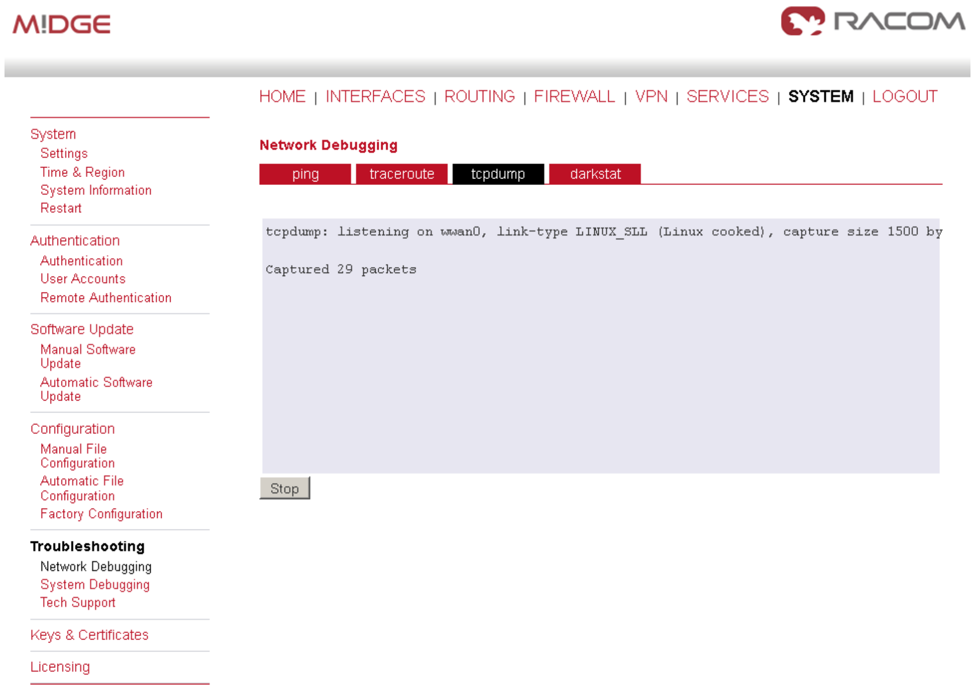
Interface: WWAN1

Exclude:
□ http
□ https
□ telnet
□ ssh

Rys.: Wybór interfejsu do skanowania

Analizę ruchu możemy przeprowadzać na interfejsach (**interface**) WWAN, LAN1 i LAN2. Aby zmniejszyć ilość danych możemy wykluczyć (**exclude**) nie interesujące nas protokoły np. http, https, telnet, ssh. W przypadku naszego klienta monitorowaliśmy ruch na interfejsie LAN1.

Po wybraniu interfejsu który chcemy obserwować klikamy na **start**.



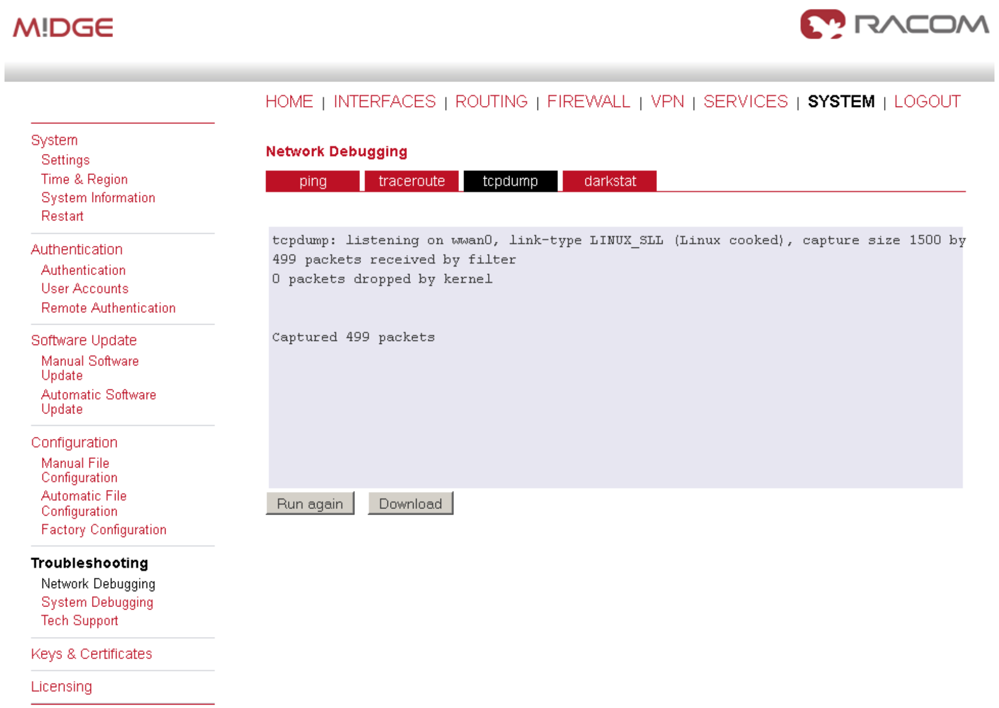
```
tcpdump: listening on wwan0, link-type LINUX_SLL (Linux cooked), capture size 1500 by

Captured 29 packets
```

Rys.: Capture

Powinniśmy zobaczyć poniższe informacje:

*tcpdump: listening on wwan0, link-type LINUX_SLL (Linux cooked), capture size 1500 bytes*

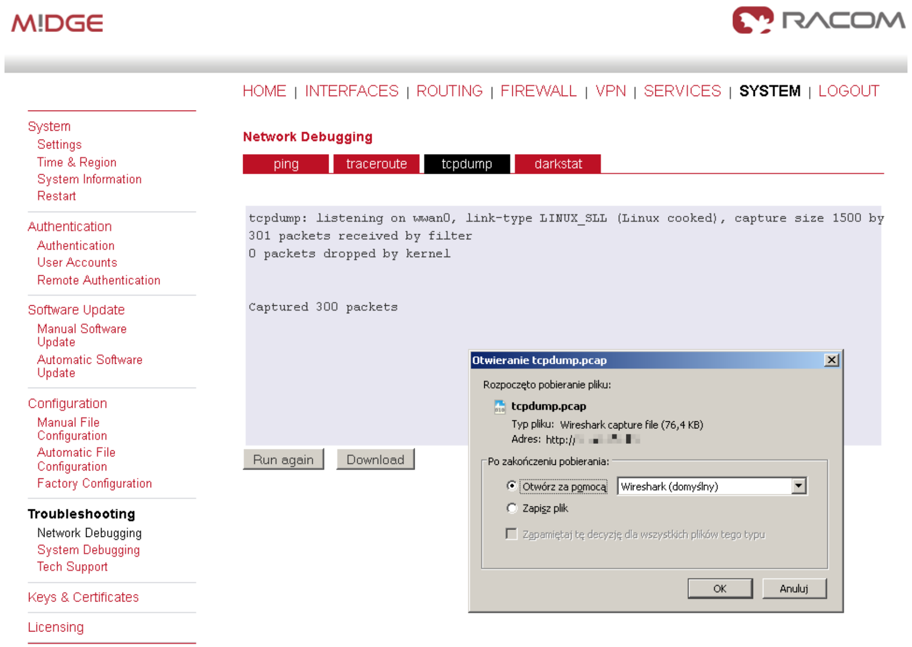
*Captured 221 packets*



```
tcpdump: listening on wwan0, link-type LINUX_SLL (Linux cooked), capture size 1500 by
499 packets received by filter
0 packets dropped by kernel


Captured 499 packets
```

Rys.: Download

Jeśli liczba przechwyconych pakietów nam odpowiada klikamy na stop, możemy teraz kliknąć na **download** i pobrać plik przechwytywania, ma o nazwę „tcpdump.pcap"



```
tcpdump: listening on wwan0, link-type LINUX_SLL (Linux cooked), capture size 1500 by
301 packets received by filter
0 packets dropped by kernel


Captured 300 packets
```

Rozpoczęto pobieranie pliku:

**tcpdump.pcap**

Typ pliku: Wireshark capture file (76,4 KB)

Adres: http://[redacted]

Po zakończeniu pobierania:

● Otwórz za pomocą Wireshark (domyślny)

○ Zapisz plik

☐ Zapamiętaj tę decyzję dla wszystkich plików tego typu

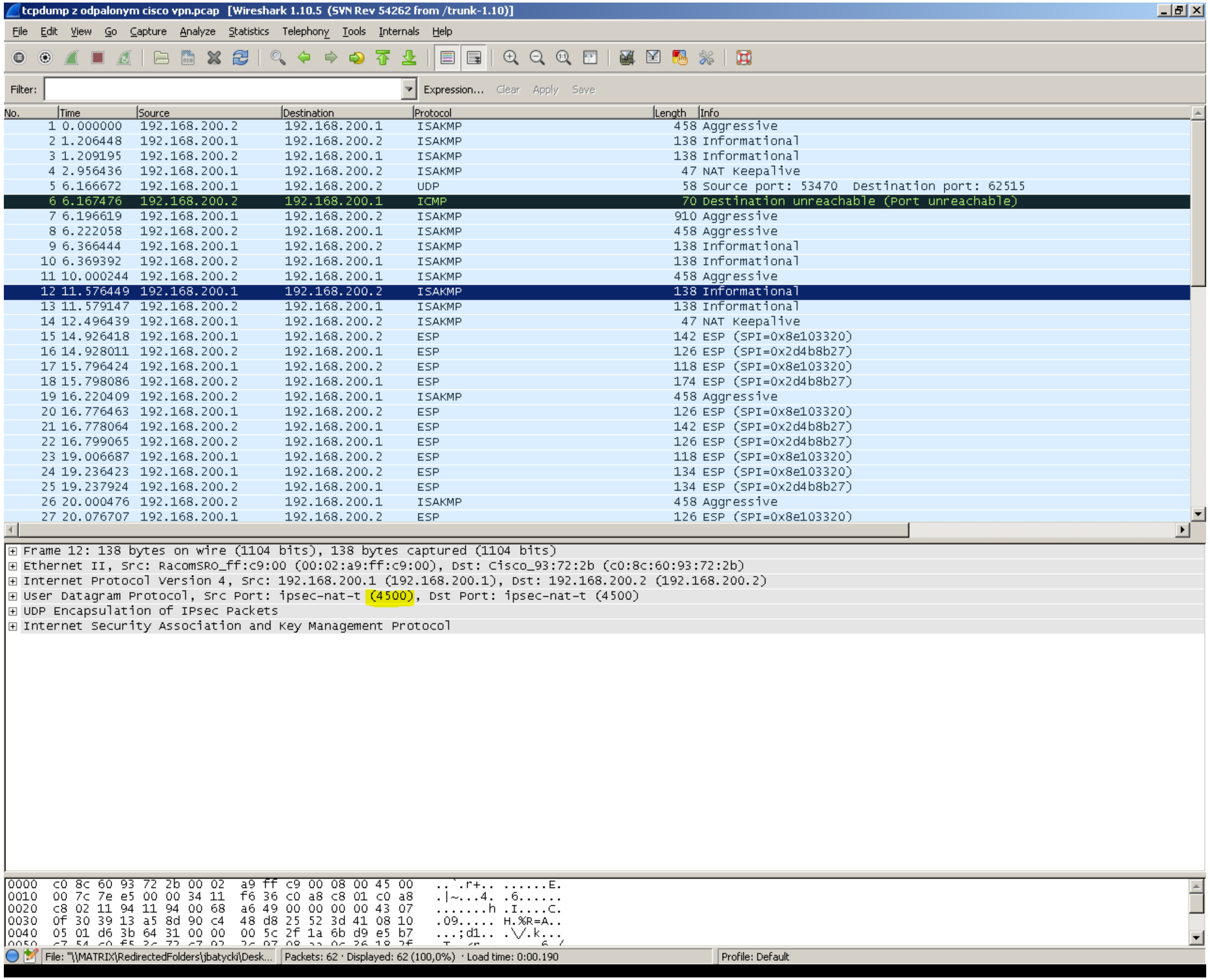
Rys.: Zapisywanie pliku do wireshark

Taki plik możemy otworzyć programem Wireshark i przystąpić do analizy. Dostępne informacje które podaje nam program to: numer, czas, źródło pakietu, cel pakietu, protokół, długość i opis:

1 0.00000041.61.144.231 25.50.116.222 TCP 1276 [TCP segment of a reassembled PDU]

Po kliknięciu na wybraną pozycję dodatkowo możemy sprawdzić np. port komunikacyjny na jakim odbywa się transmisja. Port zarówno źródłowy jak i docelowy np.:

User Datagram Protocol, Src Port: ipsec-nat-t (4500), Dst Port: ipsec-nat-t (4500)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: 53471 (53471)



tcpdump z odpalonym cisco vpn.pcap [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

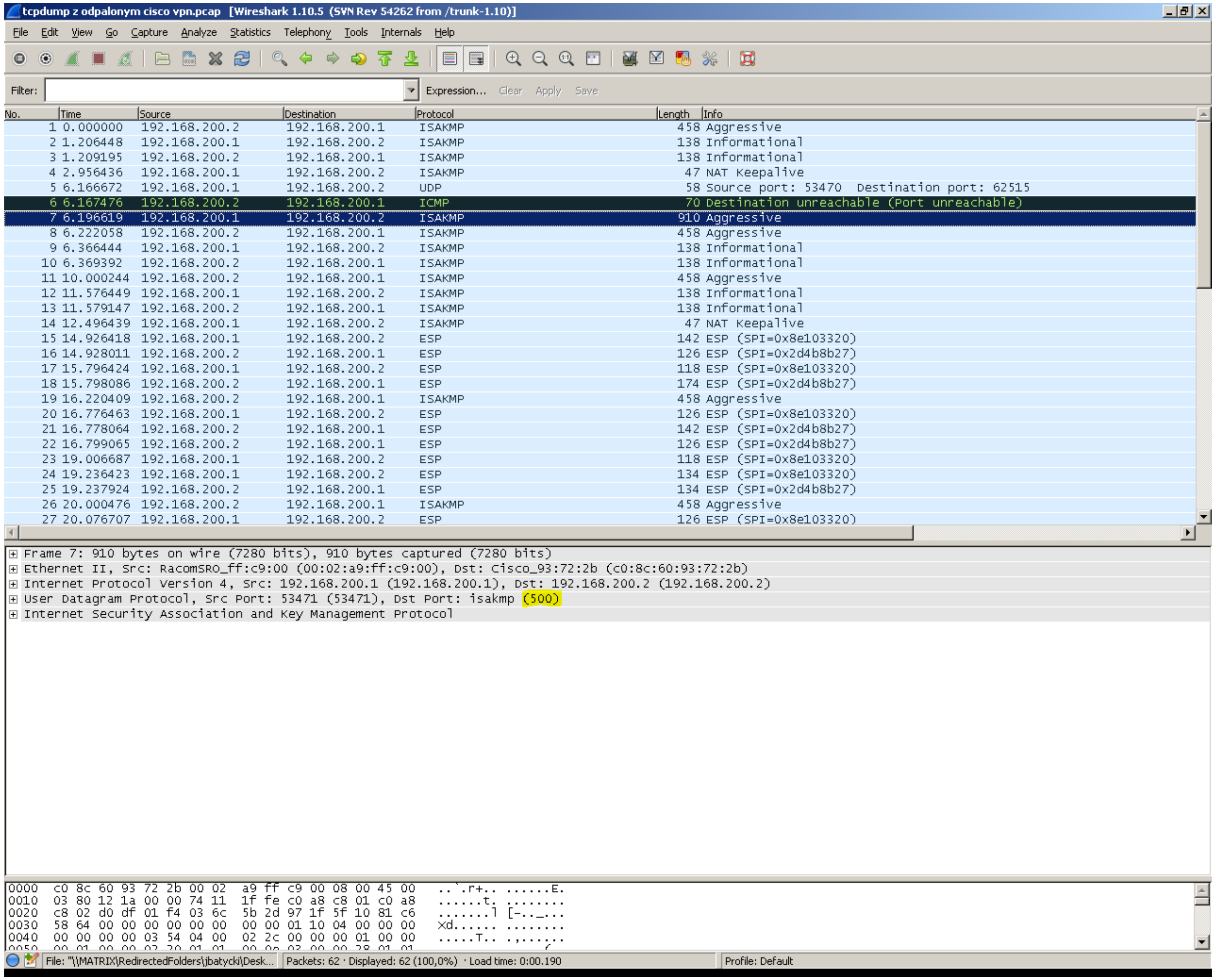
```
No.  Time      Source         Destination    Protocol  Length Info
  1 0.000000   192.168.200.2  192.168.200.1  ISAKMP       458 Aggressive
  2 1.206448   192.168.200.1  192.168.200.2  ISAKMP       138 Informational
  3 1.209195   192.168.200.2  192.168.200.1  ISAKMP       138 Informational
  4 2.956436   192.168.200.1  192.168.200.2  ISAKMP        47 NAT Keepalive
  5 6.166672   192.168.200.1  192.168.200.2  UDP           58 Source port: 53470  Destination port: 62515
  6 6.167476   192.168.200.2  192.168.200.1  ICMP          70 Destination unreachable (Port unreachable)
  7 6.196619   192.168.200.1  192.168.200.2  ISAKMP       910 Aggressive
  8 6.222058   192.168.200.2  192.168.200.1  ISAKMP       458 Aggressive
  9 6.366444   192.168.200.1  192.168.200.2  ISAKMP       138 Informational
 10 6.369392   192.168.200.2  192.168.200.1  ISAKMP       138 Informational
 11 10.000244  192.168.200.2  192.168.200.1  ISAKMP       458 Aggressive
 12 11.576449  192.168.200.1  192.168.200.2  ISAKMP       138 Informational
 13 11.579147  192.168.200.2  192.168.200.1  ISAKMP       138 Informational
 14 12.496439  192.168.200.1  192.168.200.2  ISAKMP        47 NAT Keepalive
 15 14.926418  192.168.200.1  192.168.200.2  ESP          142 ESP (SPI=0x8e103320)
 16 14.928011  192.168.200.2  192.168.200.1  ESP          126 ESP (SPI=0x2d4b8b27)
 17 15.796424  192.168.200.1  192.168.200.2  ESP          118 ESP (SPI=0x8e103320)
 18 15.798086  192.168.200.2  192.168.200.1  ESP          174 ESP (SPI=0x2d4b8b27)
 19 16.220409  192.168.200.2  192.168.200.1  ISAKMP       458 Aggressive
 20 16.776463  192.168.200.1  192.168.200.2  ESP          126 ESP (SPI=0x8e103320)
 21 16.778064  192.168.200.2  192.168.200.1  ESP          142 ESP (SPI=0x2d4b8b27)
 22 16.799065  192.168.200.2  192.168.200.1  ESP          126 ESP (SPI=0x2d4b8b27)
 23 19.006687  192.168.200.1  192.168.200.2  ESP          118 ESP (SPI=0x8e103320)
 24 19.236423  192.168.200.1  192.168.200.2  ESP          134 ESP (SPI=0x8e103320)
 25 19.237924  192.168.200.2  192.168.200.1  ESP          134 ESP (SPI=0x2d4b8b27)
 26 20.000476  192.168.200.2  192.168.200.1  ISAKMP       458 Aggressive
 27 20.076707  192.168.200.1  192.168.200.2  ESP          126 ESP (SPI=0x8e103320)
```

```
⊞ Frame 12: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits)
⊞ Ethernet II, Src: RacomSRO_ff:c9:00 (00:02:a9:ff:c9:00), Dst: Cisco_93:72:2b (c0:8c:60:93:72:2b)
⊞ Internet Protocol Version 4, Src: 192.168.200.1 (192.168.200.1), Dst: 192.168.200.2 (192.168.200.2)
⊞ User Datagram Protocol, Src Port: ipsec-nat-t (4500), Dst Port: ipsec-nat-t (4500)
⊞ UDP Encapsulation of IPsec Packets
⊞ Internet Security Association and Key Management Protocol
```

```
0000  c0 8c 60 93 72 2b 00 02  a9 ff c9 00 08 00 45 00   ..`.r+.. ......E.
0010  00 7c 7e e5 00 00 34 11  f6 36 c0 a8 c8 01 c0 a8   .|~...4. .6......
0020  c8 02 11 94 11 94 00 68  a6 49 00 00 00 00 43 07   .......h .I....C.
0030  0f 30 39 13 a5 8d 90 c4  48 d8 25 52 3d 41 08 10   .09..... H.%R=A..
0040  05 01 d6 3b 64 31 00 00  00 5c 2f 1a 6b d9 e5 b7   ...;d1.. .\/.k...
```

File: "\\MATRIX\RedirectedFolders\jbatycki\Desk... Packets: 62 · Displayed: 62 (100,0%) · Load time: 0:00.190 Profile: Default

Rys.: Wireshark analiza



tcpdump z odpalonym cisco vpn.pcap  [Wireshark 1.10.5  (SVN Rev 54262 from /trunk-1.10)]

```
No.  Time       Source          Destination     Protocol   Length Info
   1 0.000000   192.168.200.2   192.168.200.1   ISAKMP        458 Aggressive
   2 1.206448   192.168.200.1   192.168.200.2   ISAKMP        138 Informational
   3 1.209195   192.168.200.2   192.168.200.1   ISAKMP        138 Informational
   4 2.956436   192.168.200.1   192.168.200.2   ISAKMP         47 NAT Keepalive
   5 6.166672   192.168.200.1   192.168.200.2   UDP            58 Source port: 53470  Destination port: 62515
   6 6.167476   192.168.200.2   192.168.200.1   ICMP           70 Destination unreachable (Port unreachable)
   7 6.196619   192.168.200.1   192.168.200.2   ISAKMP        910 Aggressive
   8 6.222058   192.168.200.2   192.168.200.1   ISAKMP        458 Aggressive
   9 6.366444   192.168.200.1   192.168.200.2   ISAKMP        138 Informational
  10 6.369392   192.168.200.2   192.168.200.1   ISAKMP        138 Informational
  11 10.000244  192.168.200.2   192.168.200.1   ISAKMP        458 Aggressive
  12 11.576449  192.168.200.1   192.168.200.2   ISAKMP        138 Informational
  13 11.579147  192.168.200.2   192.168.200.1   ISAKMP        138 Informational
  14 12.496439  192.168.200.1   192.168.200.2   ISAKMP         47 NAT Keepalive
  15 14.926418  192.168.200.1   192.168.200.2   ESP           142 ESP (SPI=0x8e103320)
  16 14.928011  192.168.200.2   192.168.200.1   ESP           126 ESP (SPI=0x2d4b8b27)
  17 15.796424  192.168.200.1   192.168.200.2   ESP           118 ESP (SPI=0x8e103320)
  18 15.798086  192.168.200.2   192.168.200.1   ESP           174 ESP (SPI=0x2d4b8b27)
  19 16.220409  192.168.200.2   192.168.200.1   ISAKMP        458 Aggressive
  20 16.776463  192.168.200.1   192.168.200.2   ESP           126 ESP (SPI=0x8e103320)
  21 16.778064  192.168.200.2   192.168.200.1   ESP           142 ESP (SPI=0x2d4b8b27)
  22 16.799065  192.168.200.2   192.168.200.1   ESP           126 ESP (SPI=0x2d4b8b27)
  23 19.006687  192.168.200.1   192.168.200.2   ESP           118 ESP (SPI=0x8e103320)
  24 19.236423  192.168.200.1   192.168.200.2   ESP           134 ESP (SPI=0x8e103320)
  25 19.237924  192.168.200.2   192.168.200.1   ESP           134 ESP (SPI=0x2d4b8b27)
  26 20.000476  192.168.200.2   192.168.200.1   ISAKMP        458 Aggressive
  27 20.076707  192.168.200.1   192.168.200.2   ESP           126 ESP (SPI=0x8e103320)
```

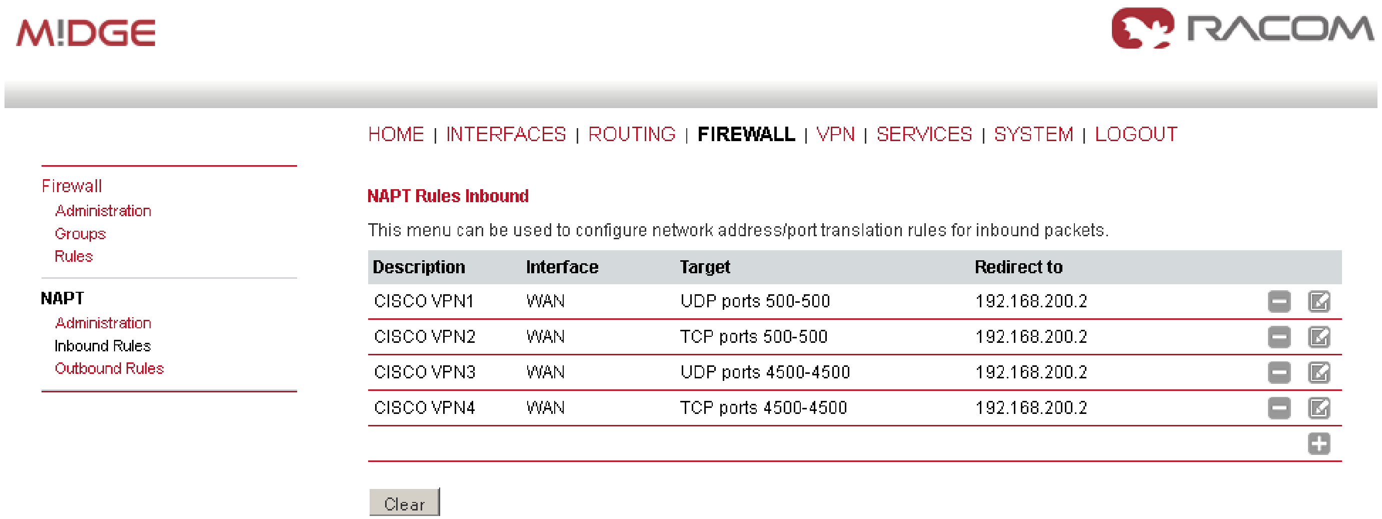
```
⊞ Frame 7: 910 bytes on wire (7280 bits), 910 bytes captured (7280 bits)
⊞ Ethernet II, Src: RacomSRO_ff:c9:00 (00:02:a9:ff:c9:00), Dst: Cisco_93:72:2b (c0:8c:60:93:72:2b)
⊞ Internet Protocol Version 4, Src: 192.168.200.1 (192.168.200.1), Dst: 192.168.200.2 (192.168.200.2)
⊞ User Datagram Protocol, Src Port: 53471 (53471), Dst Port: isakmp (500)
⊞ Internet Security Association and Key Management Protocol
```

```
0000  c0 8c 60 93 72 2b 00 02  a9 ff c9 00 08 00 45 00   ..`.r+.. ......E.
0010  03 80 12 1a 00 00 74 11  1f fe c0 a8 c8 01 c0 a8   ......t. ........
0020  c8 02 d0 df 01 f4 03 6c  5b 2d 97 1f 5f 10 81 c6   .......l [-.._...
0030  58 64 00 00 00 00 00 00  00 00 01 10 04 00 00 00   Xd...... ........
0040  00 00 00 00 03 54 04 00  02 2c 00 00 00 01 00 00   .....T.. .,......
```

File: "\\MATRIX\RedirectedFolders\jbatycki\Desk... | Packets: 62 · Displayed: 62 (100,0%) · Load time: 0:00.190 | Profile: Default

Rys.: Wireshark analiza cd.

Dzięki powyższej analizie ustaliśmy że porty które należy przekierować to: 500 i 4500
poniżej przykład przekierowania ruchu z WAN na odpowiednie IP w LAN.



NAPT Rules Inbound

This menu can be used to configure network address/port translation rules for inbound packets.

| Description | Interface | Target | Redirect to |
|---|---|---|---|
| CISCO VPN1 | WAN | UDP ports 500-500 | 192.168.200.2 |
| CISCO VPN2 | WAN | TCP ports 500-500 | 192.168.200.2 |
| CISCO VPN3 | WAN | UDP ports 4500-4500 | 192.168.200.2 |
| CISCO VPN4 | WAN | TCP ports 4500-4500 | 192.168.200.2 |

Rys.: Przykładowe przekierowanie portów